Intel Developer Update is Intel's monthly online news magazine for developers. As the official publication of developer.intel.com, it brings hardware, software, and Web developers the latest information on initiatives, technologies, platforms, and products based on the Intel® Architecture.

Cover Story

Each month, we run a cover story on the most significant industry announcement, trend, or development for the month.

Featured Articles

Delivering in-depth reports on key platforms, products and technologies, our featured articles provide a monthly source of information on issues affecting developers. Be sure to check in every month for the latest developments driving the evolution of the industry.

Contact the Editor

To make *Intel Developer Update* a better information resource, we invite you to share your thoughts on what we've published or what you'd like to see covered. Comments are always welcome.

Archives

Our archives contain two groups of previously published articles. One group contains all the articles that appeared in *Platform Solutions News*, the earlier version of *Intel Developer Update*. The articles date from September 1997 through August 1999. The other group is set up to contain *Intel Developer Update* articles dating from the inaugural September/October 1999 issue and is accessible beginning November 1999.

Bookmarking

We advise against bookmarking article pages. They're accessible online only during the month the issue is live. Thereafter, they're removed to our archives. Instead, we suggest that you bookmark the PDF (Adobe* Portable Document Format) file versions of the articles. You'll find buttons for the PDF files labeled "print article" in the right navigation section of each article. A PDF for the entire issue is labeled "print magazine" and is located near top right side of the IDU home page.

On behalf of all of us at Intel Developer Update, welcome to the future of the PC platform!

DISCLAIMER: THE MATERIALS ARE PROVIDED "AS IS" WITHOUT ANY EXPRESS OR IMPLIED WARRANTY OF ANY KIND INCLUDING WARRANTIES OF MERCHANTABILITY, NONINFRINGEMENT OF INTELLECTUAL PROPERTY, OR FITNESS FOR ANY PARTICULAR PURPOSE. IN NO EVENT SHALL INTEL OR ITS SUPPLIERS BE LIABLE FOR ANY DAMAGES WHATSOEVER (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION, LOSS OF INFORMATION) ARISING OUT OF THE USE OF OR INABILITY TO USE THE MATERIALS, EVEN IF INTEL HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. BECAUSE SOME JURISDICTIONS PROHIBIT THE EXCLUSION OR LIMITATION OF LIABILITY FOR CONSEQUENTIAL OR INCIDENTAL DAMAGES, THE ABOVE LIMITATION MAY NOT APPLY TO YOU. INTEL FURTHER DOES NOT WARRANT THE ACCURACY OR COMPLETENESS OF THE INFORMATION, TEXT, GRAPHICS, LINKS OR OTHER ITEMS CONTAINED WITHIN THESE MATERIALS. INTEL MAY MAKE CHANGES TO THESE MATERIALS, OR TO THE PRODUCTS DESCRIBED THEREIN, AT ANY TIME WITHOUT NOTICE. INTEL MAKES NO COMMITMENT TO UPDATE THE MATERIALS.

Copyright © Intel Corporation 1999. *Third-party brands and names are the property of their respective owners.

Table of Contents

(Click on page number to jump to articles)

Note: Intel does not control the content on other company's Web sites or endorse other companies supplying products or services. Any links that take you off of Intel's Web site are provided for your convenience.

Copyright © Intel Corporation 1999. *Third-party brands and names are the property of their respective owners.

Cover Story

Intel's New 820 Chipset: System Bandwidth for the PC Platform

Joe Van De Water
Product Marketing Manager
Platform Components Group
Intel Corporation

Overview

The astounding growth of the Internet has placed new demands on the PC platform. That's because the emerging wave of today's and tomorrow's content-rich, online applications require much higher system bandwidth compared with older applications such as word processors and office suites.

While faster CPUs and graphics accelerators are being introduced to the market to handle the demands of these next generation applications, developers also require next generation chipset technology capable of delivering the concurrent bandwidth and low-loaded latency to keep pace. Enter the latest chipset from Intel designed to meet the challenge: the Intel® 820 chipset.

Featuring such innovations as the new Intel® Accelerated Hub Architecture, high-speed RDRAM* memory, and AGP 4X technology for advanced graphics performance, the Intel 820 chipset is targeted at the next wave of Intel® Pentium® III processor-based mainstream and performance PCs. Keeping in step with the newest generation of Pentium III processors introduced on October 25, the Intel 820 chipset features a high-speed 133-MHz system bus and has been tuned to take advantage of the latest advances in the Intel® Architecture.

Headroom for the Future

The Intel 820 chipset significantly improves user experiences in Pentium III processor-based platform applications by offering more efficient allocation of system resources, increased bandwidth, and greater functionality. The new chipset is the first to utilize the combination of RDRAM memory technology, a 133-MHz system bus, and significant graphic performance enhancements using the 4X capability of the AGP 2.0 interface specification. As a result of these innovations, the Intel 820 chipset provides developers with the performance required to meet the needs of today's most advanced applications, along with the headroom necessary to accommodate the needs of tomorrow's next generation applications as well.

There are three primary components in the Intel 820 chipset:

- 82820 Memory Controller Hub—provides the CPU interface, DRAM interface, and AGP interface for the platform while providing support for single or dual processors
- 82801 I/O Controller Hub—utilizes the Intel Accelerated Hub Architecture to make a direct connection from the graphics and memory to an integrated AC97 controller, ATA66 controller, dual USB ports, and PCI add-in cards
- Firmware Hub—stores system BIOS and video BIOS, as well as the Intel® Random Number Generator, which enables stronger encryption, digital signatures, and security protocols

Copyright © Intel Corporation 1999. *Third-party brands and names are the property of their respective owners.

In the Forefront

The Intel 820 chipset uses a 133-MHz processor system bus, which offers developers a much higher degree of system bus flexibility. This new bus raises the processor-to-memory and graphics bandwidth from today's top speed of 800 megabytes per second to a full 1 gigabyte (GB)/second.

The new chipset also incorporates the Intel-Accelerated Hub Architecture, which at 266 MB/second provides twice the bandwidth of the PCI bus. This allows a much wider flow of content-rich application information from the I/O controller to its memory counterpart, providing optimized arbitration rules that enable more functions to run concurrently and pave the way for more lifelike audio and video on the PC platform.

Another innovation featured in the Intel 820 chipset is RDRAM technology, which is capable of delivering twice the peak memory bandwidth—and up to three times the effective memory bandwidth—of today's 100-MHz SDRAM systems. Providing data throughput of up to 1.6 GB/second, RDRAM allows many more memory pages to be open, which in turn increases the opportunity for page hits and better memory access. For end users, it all translates into better concurrent processing, richer 3D graphics, and better system responsiveness.

Advanced Graphics Performance

The Intel 820 chipset utilizes an AGP 4X interface that allows graphics controllers to access main memory at more than 1 GB/second—effectively doubling the graphics bandwidth provided by existing AGP 2X implementations and enabling PCs to render larger-textured 3D images faster than ever before.

The new chipset also offers a number of other important features that will enable developers to expand the envelope of PC performance. An ATA66 controller provides a doubling of available bandwidth to hard disk drives. The Intel Random Number Generator boosts data protection through encryption. The Alert on LAN* 1.0 can emit an alert in case of software failure or system intrusion to the system administrator, even when the operating system is not present or the system is suspended. And the low pin-count (LPC) interface removes the need for the legacy ISA expansion bus, providing cost, space savings, and improving system reliability. Together these features help pave the way for new PC form factors and an improved Internet experience.

Summary

Scalability and flexibility are key attributes of the Intel 820 chipset, which now joins the recently introduced Intel® 810E and Intel® 840 chipsets as part of Intel's new generation of chipset solutions optimized for Pentium III processor-based platforms.

Incorporating many of the technological innovations of the Intel 820 chipset, the Intel 810E differs principally from its higher-performance counterpart by utilizing 100-MHz SDRAM technology instead of RDRAM, and by providing support for one processor instead of two. And the Intel 840 chipset, based on Intel® Scalable Bandwidth Technology, is Intel's first chipset designed specifically to meet the needs of the workstation platform.

The new Intel 820 chipset, however, stands alone as the Intel solution of choice for high-performance PCs. It paves the way for new levels in system performance, flexibility and stability, making the Internet and its content-rich applications more accessible and dynamic for end users everywhere. In combination with Intel's other chipsets, it all translates into more and better choices than ever for system developers and their customers, spanning all price/performance points on the PC platform.

Copyright © Intel Corporation 1999. *Third-party brands and names are the property of their respective owners.

More Info

For more information on the Intel® 820 chipset, visit our Web sites at:

- Chipsets
- 820 Chipset Product Overview
- Intel 820 Chipset Demo

For more information on Intel Desktop Boards featuring the 820 chipset, visit our Web sites listed below. Be sure to visit our next issue for a more indepth article on desktop boards.

- Intel Desktop Boards
- Intel® Desktop Board VC820
- Intel® Desktop Board CC820
- Desktop Board Press Release

Author Bio

Joe Van De Water is desktop chipset marketing manager for Intel Corporation's Platform Components Group. Joe has worked at Intel for the past seven years, holding several positions within the Platform Components Group ranging from product planning to product marketing. Prior to Intel, Joe worked as a manufacturing engineer at Raychem Corporation. He holds a Bachelor of Science degree as well as a Master’s in industrial engineering from Stanford University.

Copyright © Intel Corporation 1999. *Third-party brands and names are the property of their respective owners.

Columns

Inside Looking In

Is Collateral Worth What You Pay?

Tim Mostad
Senior Technical
Marketing Manager
Intel Corporation

Column

Intel engineers produce mountains of technical collateral including presentations, white papers, design guides, training classes, reference designs, and performance analyses. The vast majority of it is given away freely with the exception of documents containing some kind of sensitive information. Even then there's no charge.

You can bet that every writer envisions his or her document making a difference. Maybe not solving world hunger, but touching just the right audience with that ever-so-crucial piece of information. The writers imagine that their experiences and learning will save someone time or money if they can only get the information in enough hands or in front of enough eyes.

I know this feeling well. In my nearly two decades here, I've created dozens of such masterpieces, each time feeling like a proud parent ready to send my grown child off to change the world. By now I must have done some good for someone somewhere, right? Maybe not.

We're all so bombarded with masses of information, data which expands exponentially, that we spend a lot of time trying to organize our lives and train our brains to filter out the noise. These filters are unique to each of us. They're so effective and so personal that we're often unaware of them. Everyone has had the experience of missing a road sign or overlooking something that should have been obvious. The problem is that I cannot possibly write information that won't be filtered by the people that I want to reach the most. In retrospect, if any of my communications made a measurable difference it may have been by luck.

The challenge is to get into my audience's focus past the filters that identify noise and get them to focus on the right things—my things. Last month I wrote about value as a mechanism to connect source and destination, and I postulated that value is measured in dollars. However, we really can't expect anyone to pay for apparently Intel-serving information. But just because we can't assign dollar value to collateral doesn't mean it is worthless. In most cases, information sharing is more of a "push" process. It aims to satisfy needs that users often don't even know they have. The ultimate goal is to guide users to superior solutions influenced by ideas—my ideas. This has intrinsic value to my customers and me.

An obvious way to get my great ideas to my audience is to use the web. The web solves the universal access problem. It can get the eyeballs on my material that I desperately need but in doing so, it also amplifies the information noise level. The problem gets a lot better and much worse at the same time.

Fortunately, there are tools that offer promise. We didn't invent them, but we'll employ both personalization and intelligent data management to address the need for information filtering as we develop our own software developer Web site.

Copyright © Intel Corporation 1999. *Third-party brands and names are the property of their respective owners.

Personalization uses a registration process to capture users' interests so that they are presented information that most likely suits them. We use their self-identified concerns to pre-filter out the noise. All of the same information is still there but a guess at what the user wants is presented based on hints previously supplied. The likelihood of seeing the right kind of information upon first access improves dramatically but is not perfect so some kind of search capability is also needed.

An intelligent data management system, sometimes referred to as a knowledge base, structures information to give back the most relevant information to the user based on a search. Information is grouped by relevance so that one match also generates other leads. The user can then follow the trail until hopefully an answer is found. The knowledge base should automatically strengthen ties that are frequently used and weaken others causing the most commonly followed path to be prominently displayed to the searcher. It's not a new idea by any means but it's becoming affordable and with the increasing commotion generated by the Internet, it is becoming a necessity.

However, automation can take us just so far. In the days of print, collateral always came with a huge amount of context. Readers would not need to seek out other documents to understand what they were reading. Now this context is just more racket. Writers now must push the limits of context-less writing—just supply the facts and be as brief as possible. Our online publications need to use these facts to get straight to the point and then rely on other sources to paint the whole picture. The real work is in providing the appropriate links so that context can be derived based on the user's perspective.

Collateral is clearly worthless if we use the old methods of the past, especially if we merely throw it on the Internet worldwide wall and hope it sticks. When it simply hits the Web, collateral is instantly transformed into noise. If we take the time to build the right information infrastructure and then focus and simplify our content then we have a chance of helping at least someone, increasingly the people we want and in the way we want.

Now, if you happen to find a way to determine that the person who read your online collateral actually did what you told him or her to do, let me know. Better yet, if you write something explaining what *not* to do and you figure out a way to measure what *didn't* happen, give me a call. I might just want to write a paper that we can post on our Web site.

Author Bio

Tim Mostad continues to pursue technical marketing nirvana by applying his 19 years of Intel hardware experience to extending Intel's influence with software and Internet developers. As Operations Manager in Intel's Developer Relations Division, Tim focuses on the development of broad and efficient enabling processes and infrastructure, primarily through use of the Internet.

Copyright © Intel Corporation 1999. *Third-party brands and names are the property of their respective owners.

From the Editor

Donna Loveland
Managing Editor
Platform Marketing
Intel Corporation

Column

If Letters to the Editor are a valid indicator of your interest, you're going to be very pleased to see this month's cover story on the Intel® 820 chipset.

Over the last few weeks, you've been filling my inbox with questions about the Intel 820 chipset's features and capabilities, which include a faster processor system bus, superior memory capabilities and enhanced graphics functionality. At last, the news is public and you can get it here.

Our cover story summarizes high-performance Direct RDRAM* memory technology, AGP 4X graphics support, and the rest of the feature set. For detailed answers to those volumes of questions you've been asking about capability, availability, and more, click on the story's links to topic-specific areas of developer.intel.com.

Want more on innovation in desktop computing? Check out our piece on the latest Concept PCs just showcased at Comdex. The "article" is an animated stroll through an online gallery of machines. You can let the images scroll across your screen, or you can select individual PCs to get richly colored views complete with product descriptions.

Rounding out the December issue are three equally important text-based articles:

- ***Dual-Plane Wireless Systems Support 3G Services*—**New developments in flash memory architecture and flash software data management support the persistent information storage requirements of 3G data technologies at higher data rates, and they're available now.

- ***You Can Help Define the Baseline for Trusted Computing*—**By joining the Trusted Computing Platform Alliance, you can help define the baseline for the trusted PC platform to assure the future of e-Business on the Internet.

- ***How IHVs Can Fast-Track IA-64 Drivers*—**Learn how Intel's Fast Track Program is helping IHV's port device drivers in time for the debut of systems based on the Intel® Itanium™ processor.

I welcome you to continue sending those emails. In fact, I encourage you to let me know how articles like these—and the magazine on the whole—is serving your need for information about designing and developing products based on Intel® Architecture.

Author Bio

Donna Loveland is the editor of *Intel Developer Update*. She joined Intel's Platform Marketing group earlier this year as the editor of *Platform Solutions News*. Donna began her high-tech career with Intel in 1982 as a technical editor in an advanced microprocessor development group. Since then, she's held technical and marketing positions related to leading-edge technologies in areas ranging from stereoscopic display to digital broadcast to scalable online content. She holds a BA degree in English from the University of Rochester and an MA in Expository Writing from the University of Iowa.

Copyright © Intel Corporation 1999. *Third-party brands and names are the property of their respective owners.

Departments

Applied Computing

Dual-Plane Wireless Systems Support 3G Services

Charles Brown
Wireless Marketing Program Manager
Flash Products Division
Intel Corporation

Overview

Over the next few years, cellular networks will deploy new high-speed wireless data technologies that will not only increase data throughput, but also enable new applications and services. Applications such as mobile navigation and other services using maps and graphics will benefit greatly from the enhancement throughput provided by this technology. Users will be capable of remote network and Internet access as if they where connected in their office, making the data enriched phone more attractive and easier to use.

Third-generation (3G), high-speed wireless data technologies will require new handsets to support the enhanced signal processing and a reliable means to store the new information created by the many new applications. This information may be stored on a network server or locally in the handset. There are issues with storing information on the server, namely the time delay to access the information as well as out-of-coverage access. In many instances, it is desirable to store personal information persistently on the device. Timely access to this information makes the handset a more attractive and useful tool.

Handset designers are using flash memory today for persistent storage of user data in addition to the system code. They have turned to software data management techniques, such as the Intel® Flash Data Integrator (FDI) to manage this information. The increased data rates and new data structures promised by next generation cellular networks will place even greater demands on the memory performance and data manager. New developments in flash memory architecture and flash software data management are now available to support persistent information storage requirements of 3G data technologies at higher data rates.

The Quantum Leap

High-speed circuit-switched data (HSCSD) and general packet radio services (GPRS) are two new methods that will provide cellular phone users new services such as image transfer, remote local-area network LAN access, Internet access, and more. These new technologies put wireless data rates on par with wireline service, and may mark the dawn of the wireless Internet. Current applications, such as e-mail and remote LAN access, as well as new applications, such as wireless imaging and video, will benefit from higher bit rates.

HSCSD provides data throughput six times faster than that of current wireless data with only minor network software upgrades. This employs a new coding scheme and the ability to combine time slots so that data rates in multiples of 9.6 kb/s or 14.4 kb/s are possible. This means users will be provided with a variety of new data rates, ranging from 9.6 kb/s to 57.6 kb/s.

GPRS, on the other hand, will enable new applications not previously feasible over cellular networks, offering more attractive wireless Internet access. With GPRS, data is encapsulated into individual packets and transmitted over the network. Network capacity is allocated only when data is being sent. Network resources are released as soon as it is no longer needed, after the packet has been sent, providing immediate connectivity and high throughput. GPRS offers a very flexible range of bit rates, from less than 100 b/s to over 100 kb/s. Using links in this way provides for lower cost data service, since network capacity is conserved. Users are charged for the amount of data sent or received, not the time connected to the network. A host of new applications will be within reach with GPRS, including: remote access to business IP networks, mobile credit card verification, electronic commerce, and any number of new data services.

Copyright © Intel Corporation 1999. *Third-party brands and names are the property of their respective owners.

Persistent Data Storage Considerations

Understanding the attributes of these new data connection methods provides insight into the design of the data storage system. HSCSD provides a constant rate data channel that is capable of sending and receiving a continuous stream of data. The handset terminal typically is unaware of the amount of information that needs to store. The amount of available memory and the rate at which information can be stored are essential elements in the design of a robust memory manager.

The circuit switched data manager must accommodate the storage of variable size data structures with unknown length such as data files or digital audio messages. To accomplish this, a free block of memory is required to allow for incoming data to be stored while the system reclaims (erases) old information in preparation for the storage of more incoming data.

An alternative caching method, where the information is buffered in system memory, has been an effective way for computers to manage such information storage. Although a caching architecture is less than efficient for handsets with limited space, budget and power constraints and does not provide a reliable storage method in the event of power loss. As a result, designers have turned to directly storing the information into flash memory.

The software data manager handles the direct storage of a stream of data into flash memory. The system must provide a means to specify which old information may be reclaimed in the event the amount of incoming data exceeds the amount of free memory space. The process of constantly checking for available memory requires background erase operation to allow for reclaiming of old data while receiving new data.

Chart 1 illustrates the basic concept of managing a circuit switched connection. New data received is appended to a file structure until the entire contents have been stored. A reliable persistent storage manager for HSCSD must reclaim memory space as data is received. Information is appended to an open file while old information is erased in the background.

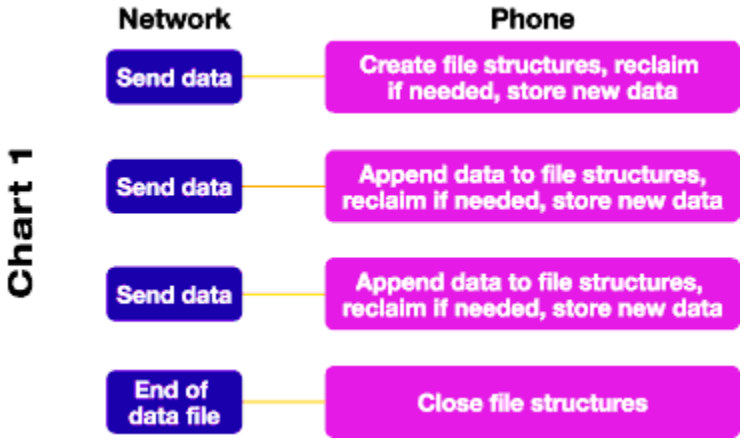

Chart 1: Managing a Circuit Switched Connection.

With GPRS, data is arranged into small packets with a header containing the origin, destination address, and size of the data. The packets are then sent individually over the cellular network; packets originating from one user may take different routes through the network to the receiver. No preset time is allocated to packet transmission, and packets from the different users are interleaved so that transmission capacity is shared.

Packet data transmission provides the opportunity for the handset software data manager to prepare the storage media prior to the data being sent. Since the data size is contained in the header information, the memory data manager software can reclaim needed memory space or decline to receive the information if no free space is available.

Copyright © Intel Corporation 1999. *Third-party brands and names are the property of their respective owners.

The GPRS data manager must support a handshake communication protocol (*Chart 2*), whereby the phone acknowledges it is prepared to receive the data and the reception of the individual packets. Data packets are then rearranged into their original order according to the packet number provided in the header structure. GPRS allows the memory data manager to prepare the media ahead of time to support direct high-speed storage. A handshake protocol between the handset and data source acknowledge the phone is prepared to store the data and when the data packet is successfully received.

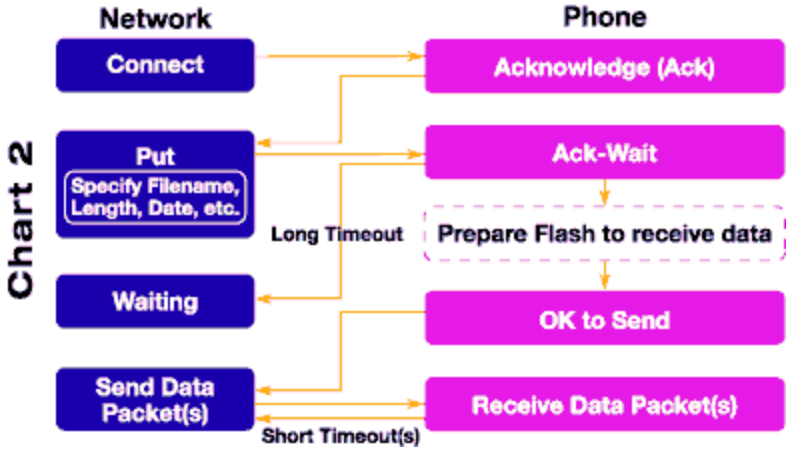

Chart 2: GPRS and the Handshake Communication Protocol.

New Dual-Plane Flash Memory

Many currently available flash memories must complete a program or erase operation before data or code can be read from another memory block. Based on the program/erase timing specifications of flash, there is a common misconception that data storage can be supported only when the application can mask interrupts and allow a flash memory write or erase operation to complete. In time-synchronized applications with latencies in the range of microseconds, such as a cellular phone, simultaneous read and write operation can be accomplished using software methods.

Enhanced suspend circuitry allow flash memory program/erase operations to be suspended temporarily to read code from another memory block. Suspend circuits allow time-critical operations to be serviced without stalling the microprocessor. Thus, providing software controlled “read-while-write” operation. Suspend circuits do not increase the flash die size (cost), thereby providing the most cost-effective solution for basic consumer phones with less demanding data storage needs such as user information, phone settings, and short message service (SMS) messages.

In anticipation of the higher data rates offered by next generation cellular, additional hardware assistance may be needed to allow an erase operation to continue uninterrupted. To accomplish this, the standard flash memory array can be segmented into separate physical planes with duplicate row and column decoders. This dual-plane flash memory (*Chart 3*) allows the system to write or erase information in one plane of the memory while at the same time the processor is reading instructions from the other plane. For example, this feature allows an erase operation to continue without delay thereby reducing the time it takes to store large data structures during a memory reclaim operation (*Chart 4*).

Copyright © Intel Corporation 1999. *Third-party brands and names are the property of their respective owners.

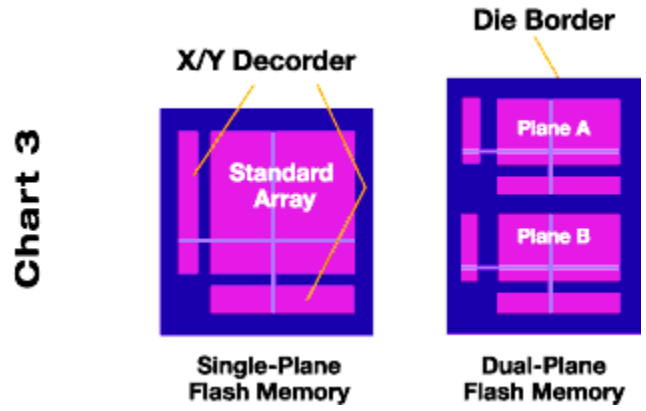

Chart 3: Increased Data Storage Throughput.

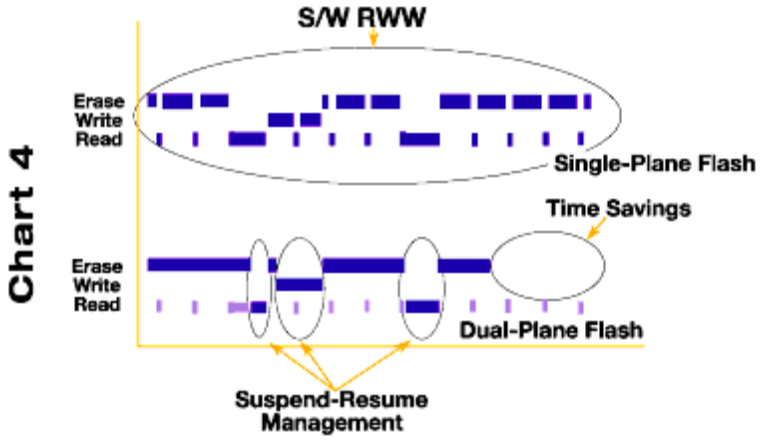

Chart 4: Simultaneous Background Erase and Code Read

Dual-plane flash memory improves data storage throughput by up to 150 percent over single plane flash memory, depending on the memory bus utilization (*Chart 5*). Such an improvement provides a solution for data rates up to hundreds of kb/s to support the evolution of wireless data services.

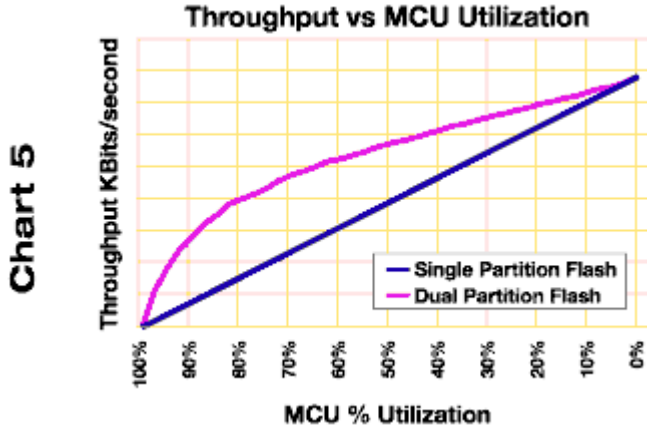

Chart 5: Up to 150 Percent Increase in Data Throughput Over Single-Plane Flash Memory

Copyright © Intel Corporation 1999. *Third-party brands and names are the property of their respective owners.

Software Needs

As with other flash products, software is needed to efficiently manage code and data in single- and dual-plane flash designs. The storage, access, and reclamation of data blocks necessitate software intervention.

The approach of data management in dual-plane flash must still support erase suspend operations in the event critical data must be written during a reclamation process. Since access to data in the same plane is necessary, the same software techniques used for software read-while-write in single-plane flash are also required for dual-plane. In addition, software is necessary to provide a common storage interface to the application.

The storage functions for next-generation handsets must accommodate a variety of data structures, including variable-size parameters, data streams, and packet data. The approach of storing data streams and packets is well understood yet intricate due to the need to handle the conditions previously described.

New extensions to software, such as Intel's FDI package, provide support for the storage of circuit switched data and data packets in single- and dual-plane flash. The designer may now choose the flash memory based on the code performance and data throughput needs of the application.

One Step Ahead

As flash memory management techniques advance, the designer must reconcile the trend toward enriched data management while also balancing cost and hardware capability. Software data managers and new dual-plane flash memory provide the designer a complete solution to accommodate future data enhancements. This capability helps designers and network operators stay one step ahead of changing market needs.

More Info

For more information on Intel® Dual-Plane Flash memory, visit our Web site:

- Intel® Dual-Plane Flash Memory
- Product Overview
- Datasheet
- Flash Memory

Author Bio

Charles Brown is a wireless marketing program manager for Intel’s Folsom, CA-based Flash Products Division. He is responsible for market research and development, as well as product planning for wireless applications of Intel’s flash memory components. Brown holds a BSEE from the University of California at Davis, an MS in Electrical Engineering from Stanford University, and a Ph.D. in Electrical Engineering from the University of California at Davis.

Copyright © Intel Corporation 1999. *Third-party brands and names are the property of their respective owners.

Initiatives and Technologies

You Can Help Define the Baseline for Trusted Computing

David Scheer
Security and Privacy Industry Marketing Manager
TCPA Program Manager
Desktop Products Group
Intel Corporation

Overview

You've heard it before. Internet e-Commerce could hit the trillion dollar level by 2003 (Forrester Research 1999). But what if security breaches, or simply perceived threats, get in the way? The open PC architecture and the infrastructure of the Internet give us the freedom to collaborate and do business, but this same openness can make us vulnerable. That's why, as the Internet grows, so does the importance of trusted computing.

The Trusted Computing Platform Alliance (TCPA) is a new working group chartered to develop a consistent baseline specification for PC security. Today we have lots of vertical security solutions, ranging from Public Key Infrastructure (PKI) and Virtual Private Networks to smart cards and biometric devices. Rather than replacing these solutions, the TCPA's goal is to define a platform specification for hardware, system software, and the operating system (OS) that can help them work better. Joining the TCPA is your opportunity to help define the emerging baseline for trusted computing.

Top-to-Bottom Security

While today's PCs already offer a level of trust to users, the growth of the Internet economy and the emergence of new connected applications puts trust and security in the spotlight. Many incremental security solutions now exist, but today's security capabilities are added-on, instead of designed-in. There are currently no PC-based system hardware standards to build trust in the platform or that provide a baseline for developers to build on.

Security on the PC is no longer just about software. Connected PC applications make security a top-to-bottom issue that involves the entire platform, including system-level hardware as well as the BIOS and operating system. The TCPA specification refers to security-related platform building blocks including protected storage, technologies for electronic signing and hashing of data, a hardware-based Intel® Random Number Generator (RNG), integrity metrics, and new OS functions.

What's Coming Up

The first-round TCPA specification release candidate was posted on the TCPA Web site November 19 and is available for review by participating members.

Objectives include:

- Enhancing the value of existing security applications, such as firewalls and Virtual Private Networks (VPNs)
- Adding value to applications that have security-related components, including Web browsers that incorporate the Secure Sockets Layer (SSL) and email applications that employ S-MIME (Secure Multipurpose Internet Mail Extensions) encoding
- Improving interoperability to make security solutions easier to develop, deploy, and use
- Permitting worldwide export, since general-purpose encryption is not part of the specification
- Providing PC owners with control over security policy, with the ability to delete any information

Copyright © Intel Corporation 1999. *Third-party brands and names are the property of their respective owners.

After review by participating members, the TCPA will announce the completed specification in mid-2000 and transfer it to an industry standards body, which remains to be selected.

How You Can Join

Compaq, HP, IBM, Intel, and Microsoft formed the Trusted Computing Platform Alliance, or TCPA, and membership is growing rapidly. TCPA membership is open to hardware and software companies with products or applications relating to security on the PC platform.

Joining the TCPA entitles your company to the following benefits:

- Participation in conferences, including the Members Meeting which is scheduled for January 16, 2000
- Participation in technical workgroups
- Invitation to participate in marketing events
- Early access to the specification
- Participation in specification development
- Your company's listing in the TCPA membership list

The TCPA is defining the future of the trusted PC to solidify this essential building block of e-Business and the Internet economy. This is your opportunity to join us, review the specification, and make your voice heard.

More Info

The TCPA Web site contains detailed information about the Trusted Computing Platform Alliance, including presentations, upcoming events, press announcements and details on how new members can join.

The Intel Security Initiative Web site provides technical information on the hardware-based Intel Random Number Generator (RNG) and other security technologies supported by Intel, including Boot Integrity Services (BIS) and IP Security. For more information on RNG, see the article entitled Increase Data Protection with the Hardware-Based Intel Random Number Generator in the *Intel Developer Update* archive.

Author Bio

In his 10 years with Intel, David Scheer has held a variety of managerial positions ranging from technical marketing to sales. He is currently the marketing manager responsible for directing security development efforts and relationships in the industry within the company's Desktop Products Group. In addition, David serves as TCPA Program Manager and as a member of the TCPA steering committee. David holds eight patents in the area of computer design and has written articles for a *EE Times*, *IEEE*, and *IC Card System and Design* and has presented in a number of technical conferences.

Copyright © Intel Corporation 1999. *Third-party brands and names are the property of their respective owners.

Servers

How IHVs Can Fast-Track IA-64 Drivers

Lauri Minas
Manager, Server Industry Marketing
Enterprise Server Group
Intel Corporation

Overview

IA-64 systems will make a huge splash, and they're coming soon. OEMs and IA-64 vendors are on track to deliver new products concurrent with production of the Intel® Itanium™ processor in mid-2000. Publicity is expected to outshine any prior IA-32 launch, and independant hardware vendors (IHVs) who can deliver products with drivers ported to IA-64 will be positioned to share the spotlight.

Itanium processor-based systems are being built by many OEM vendors and will be supported by many operating system (OS) vendors, including Win64*, Monterey 64*, and Linux* 64. This variety of vendors makes it difficult for IHVs to obtain training and tools and get their drivers tested. Intel's Fast Track Driver Development Program simplifies the process by providing one source for IA-64 technical training, development tools, development vehicles, test suites, and technical support. Intel will bring all key OS vendors and OEMs to one site for training, tool distribution, and testing. The program is free. It's simple. And many IHVs are already involved. Make your reservation now for the next Fast Track session in January.

Do a Little Math

To calculate the value of Intel's single stop program for driver development, consider this sample scenario. You want your devices available for the top three IA-64 operating systems and nine OEM platforms. In the traditional scenario for developing drivers, you'd be required to contact, negotiate, and engage with multiple on-site trips to each of these vendors. This could easily require twenty-seven (9 x 3) times the usual 5 trips per driver, or potentially a hundred and thirty-five trips. That much activity could extend driver development time anywhere from two to nine man-months. Fortunately, none of this is necessary.

With Intel's Fast Track Driver Development program, IHVs for both servers and workstations can attend a single session to get training from multiple OS vendors, receive their tools, and develop a single contact and Web site for technical support. Once drivers are written, IHVs can attend plugfests where their devices can be tested on a variety of OEM platforms, with multiple operating systems and software stacks.

Here's What You Get

Fast Track Driver Development sessions provide in-depth hands-on training and information with experts from each of the OS or OEM vendors. In addition, IHVs attending the Fast Track Driver Development program receive a Software Development Vehicle (SDV). This consists of an unfinished Itanium processor-based server with a preloaded Software Development Kit (SDK) including boot software and diagnostic utilities.

Participants also receive a Driver Development Kit (DDK) including a sample driver, libraries, and utilities from the leading operating system vendors. Documentation includes technical specifications and reference manuals for the Itanium processor and documentation for the SDV.

IHVs attending Fast Track sessions also qualify for support from Intel's Technical Support Center and one-on-one support from as assigned Intel technical marketing engineer.

A plugfest in April to May 2000 will enable IHVs to save even more time by testing their drivers with multiple server and workstation platforms at one event.

Copyright © Intel Corporation 1999. *Third-party brands and names are the property of their respective owners.

Summary

Time-to-market means time-to-money for IHVs planning to ship products for IA-64 servers and workstations. IHVs need to quickly port and validate their drivers to be ready for the mid-2000 rollout of Itanium processor systems.

Intel's Fast Track Driver Development Program helps IHVs compress months of driver development time into weeks. Detailed technical training includes an authoritative review of IA-64 architecture conducted by Intel's Itanium processor architects, in addition to operating system programming models and architecture through assembly. SDK training features guidance on IA-64 software conventions, the use of development tools in hands-on labs, and code-cleaning demonstrations for key IA-64 operating system environments.

Hands-on training, Software Development Vehicles, Software Development Kits, Driver Development Kits, tools, documentation, dedicated engineering support, and one-stop validation make Intel's Fast Track Driver Development Program a great value for IHVs.

More Info

The first Fast Track session in November drew a larger than expected turnout. A large enrollment is also expected for the January Fast Track event. Space is limited, so registrations will be taken on a first-come, first-serve basis.

For registration details, telephone Jim Yent at +(503) 677-4188 or e-mail jim.yent@intel.com

Note: A signed corporate nondisclosure agreement must be on file with Intel prior to attending the training.

Author Bio

Lauri Minas is general manager for Intel's Server Industry Marketing. In her current position, she is responsible for the strategic direction of server industry efforts for Intel, and for marketing programs of server technologies across Intel divisions.

Previously, Lauri managed Intel's Wired for Management (WfM) Initiative, a cross-industry program to improve the manageability of business and home computers, which includes the WfM Baseline Specification. She has worked at Intel for 17 years, holding various positions in marketing and management. Lauri received an MBA degree in 1992, and a BA in 1979, both from Arizona State University.

She is a three-time recipient of Intel's highest award, the Intel Achievement Award:

- 1996 for success of Wired for Management program and its effect in the industry
- 1996 for delivering standards-based manageability to the industry in Windows* 95
- 1997 for success of the Net PC and Wired for Management Baseline specifications

—End of Intel Developer Update Magazine Issue 3—

Copyright © Intel Corporation 1999. *Third-party brands and names are the property of their respective owners.